REMARKS

The Office Action mailed December 31, 2007 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Claim Status and Amendment of the Claims

Claims 1-46 are currently pending.

No claims stand allowed.

Claims 1, 11-13, 23, and 38 have been amended to further particularly point out and distinctly claim subject matter regarded as the invention. No new matter has been added.

Objections to the Claims

Claims 11 and 12 stand objected to for various informalities.[1] With this Amendment, Claims 11 and 12 have been amended accordingly. Withdrawal of the objection to the claims is respectfully requested.

The 35 U.S.C. § 101 Rejection

Claims 1-12, 35, 38-39, and 44 stand rejected as allegedly being directed to nonstatutory subject matter.[2] This rejection is respectfully traversed.

[1] Office Action mailed July 29, 2008, ¶ 6.
[2] Office Action at ¶ 7.

Claims 1 and 38

The Examiner states:

> … Regarding claims 1 and 38, they are directed to a layer 2 access device, or an apparatus comprising ports, switching fabric, and control logic, however, according to the specification (Fig 2; Par 0044), these claimed features or components can be optionally implemented in software alone. Therefore, claimed apparatus, or access device lacks any hardware or computer component, and considered to be non-statutory. See MPEP 2106.01.[3]

The Applicant respectfully disagrees. In support of the Examiner's statement, the Examiner refers to paragraph 44 of the specification, which discloses that various functions performed by the network switch of the present invention may be implemented in hardware, software, or a combination thereof. The Examiner apparently considers an implementation in software to be "purely software." However, as known to those skilled in the art, a software implementation requires processing device to execute the software instructions. Software alone cannot perform the various functions. Accordingly, without such a processing device, it cannot be said to be a software *implementation*. For at least this reason, the Applicant respectfully requests the 35 U.S.C. § 101 rejection of Claims 1 and 38 be withdrawn.

Claims 2-12, 35, 39, and 44

Claims 2-12, 35, and 44 depend from Claim 1. Claim 39 depends from Claim 38. Claims 1 and 38 being allowable, Claims 2-12, 35, 39, and 44 must also be allowable for at least the same reasons as for Claims 1 and 38.

[3] Office Action at ¶ 7.

The First 35 U.S.C. § 103 Rejection

Claims 1-34 and 44-46 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al.[4] in view of Short et al.,[5] and further in view of Tsuchiva et al.[6], among which claims 1, 13, and 23 are independent claims.[7] This rejection is respectfully traversed.

According to the Manual of Patent Examining Procedure (M.P.E.P.),

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[8]

Claim 1

Claim 1 as presently amended recites:

> A layer 2 network access device comprising:
> a plurality of input ports;
> a switching fabric for routing data received on the plurality of input ports to at least one output port; and
> control logic adapted to authenticate a physical address of a user device coupled to one of the plurality of input ports, to authenticate user information provided by a user of the user device only if the physical address is valid, and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid.

The Examiner states,

> … Kanuri et a1 teaches a layer 2 network access device for providing

[4] U.S. Patent No. 6,807,179 to Kanuri et al.
[5] U.S. Patent No. 7,194,554 to Short et al.
[6] U.S. Patent No. 7,360,086 to Tsuchiva et al.
[7] Office Action mailed December 31, 2007, ¶ 5.
[8] M.P.E.P § 2143.

network security, comprising:

a plurality of input ports (Figl, 12.22; Col3, lines 25-67; multipart switch)

a switching fabric in the layer 2 network access device for routing data received on the plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col4, lines 7-52; fayer 2 switch); and

control logic in the layer 2 network access device (Col3, line 28 to CoI 5, tine 65: the switch; MAC module; switching (rules) logic) adapted to authenticate a physical address of a user device coupled to one ofthe plurality of input ports (Col3, line 28 to Col5, line 65; matching MAC addresses).

Kanuri et al fails to teach device adapted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid.

However, Short et al discloses network security/ access device adavted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 2; (2014, starts at line 12; Col9, starts at line 8; authenticating, and restricting access based on both user id/ information, and MAC).

Furthermore, Tsuchiva et al discloses network security1 access device adapted to authenticate user information provided by a user of the user device only if the physical address is valid (Col3, lines 17-45; Col 10, lines 10-50; Col 14, lines 5-55; authenticating user with the authentication table after matching of the address1 MAC in host table); if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55); and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information; and if the user is not associated with the VLAN, assign the one of the plurality of input ports to a port default VLAN (Col 10, lines 10-50; Col 14, lines 5-55)

Tsuchiva et al, Short et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Tsuchiya et al and/ or Short et al with Kanuri to design an apparatus wherein network security/ access device utilizes both user provided authentication information, and MAC, and authenticate user information provided by a user of the user device only if the physical address is valid in order to provide a robust and improved communication control mechanism.[9]

The Applicant respectfully disagrees for the reasons set forth below.

[9] Office Action at ¶ 8.

Kanuri et al. In View Of Short et al. And Further In View Of Tsuchiva et al. Does Not Disclose To Authenticate User Information Provided By A User Of The User Device Only If The Physical Address Is Valid, And To Restrict Access To The One Of The Plurality Of Input Ports In Accordance With A User Policy Associated With The User Information Only If The User Information Is Valid

In support of the Examiner's contention that Kanuri et al. in view of Short et al. and further in view of Tsuchiva et al. discloses authenticating user information provided by a user of the user device only if the physical address is valid, the Examiner refers to two portions of the detailed description of Short et al. In both instances, the Examiner refers to a starting point in Short et al., without indicating an ending point. The Applicant respectfully submits the Examiner has not provided the level of particularity required by the Patent Rules. The Examiner is respectfully requested to indicate with particularity the particular part of the references relied upon.

The Examiner refers to "Col. 4, starts at line 12." The paragraph that includes line 12 speaks generally about maintaining attributes of a source, such as MAC address, User ID, or VLAN ID associated with the source computer from which the request for access to the network was transmitted. But nowhere does the cited portion of Short et al. disclose performing one type of authentication only if another type of authentication succeeds, let alone authenticating user information provided by a user of the user device *only if the physical address is valid* as required by Claim 1.

The Examiner also refers to "Col. 9, starts at line 8." The paragraph that includes line 8 speaks generally about a source profile including one or more names, passwords, VLAN tags, MAC addresses and other information pertinent to identify and possibly bill a source. But again, nowhere does the cited portion of Short et al. disclose performing a one type of authentication

only if another type of authentication succeeds, let alone authenticating user information provided by a user of the user device *only if the physical address is valid* as required by Claim 1.

The Examiner also refers to Tsuchiya et al. regarding the Examiner's contention that Kanuri et al. in view of Short et al. and further in view of Tsuchiva et al. discloses authenticating user information provided by a user of the user device only if the physical address is valid. The portion of Tsuchiya et al. cited by the Examiner speaks generally about creating a host table by learning a source MAC address and a source IP address of a packet, and if an entry corresponding to the source IP address is not found in the host table, prompting for a user name and password. Then a message is sent to verify the received information. Thus, in Tsuchiya et al., user authentication is performed if the source *IP* address (not a physical address) is *not* found (indicating it is invalid). In other words, the user authentication of Tsuchiya et al. is not done only if a physical address is valid as required by Claim 1. Instead, user authentication in Tsuchiya et al. is done if something *other* than the physical address (the IP address) is *invalid.*

In support of the Examiner's contention that Tsuchiya et al. discloses restricting access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid, the Examiner refers also refers to portions of Tsuchiya et al that disclose performing user authentication if something *other* than the physical address (the IP address) is *invalid.* Nowhere does the portion of Tsuchiya et al. cited by the Examiner disclose restricting access to the one of the plurality of input ports in accordance with a user policy associated with the user information *only if the user information is valid* as required by Claim 1.

And in support of the Examiner's contention that Tsuchiya et al. discloses if the user is not associated with the VLAN, assigning the one of the plurality of input ports to a port default VLAN, the Examiner refers again to Tsuchiya et al. at col. 10 lines 10-50 and col. 14 lines 5-55, which discloses performing user authentication if something *other* than the physical address (the IP address) is *invalid*. Nowhere does the portion of Tsuchiya et al. cited by the Examiner disclose a port default VLAN, let alone if the user is not associated with the VLAN, assigning the one of the plurality of input ports to a port default VLAN as required by Claim 1.

For at least these reasons, the 35 U.S.C. § 103 Rejection of Claim 1 is unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claims 13 and 23

Claim 13 is a method claim corresponding to apparatus claim 1. Claim 23 is a system claim corresponding to apparatus claim 1. Claim 1 being allowable, Claims 13 and 23 must be allowable for at least the same reasons as Claim 1.

Dependent Claims 2-12, 14-22, 24-34, and 44-46

Claims 2-12 and 44 depend from Claim 1. Claims 14-22 and 45 depend from Claim 13. Claims 24-34 and 46 depend from Claim 23. Claims 1, 13, and 23 being allowable, Claims 2-12, 14-22, 24-34, and 44-46 must also be allowable for at least the same reasons as for Claims 1, 13, and 23.

Claim 3

Claim 3 recites:

> The network access device of claim 1, wherein the control logic is adapted to authenticate the user information in accordance with an IEEE 802.1x protocol.

The Examiner states:

> ... Kanuri et al. teaches the network access device of claim 1, wherein said control logic is adapted to authenticate said user information in accordance with an IEEE 802.1x protocol (Col 3, starting at line 36: IEEE 802.3).[10]

The Applicant respectfully disagrees. In support of the Examiner's contention, the Examiner refers to a portion of Kanuri et al. that discloses sending and receiving layer 2 data packets according to the IEEE 802.3 protocol. The IEEE 802.1X protocol enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless LANs.[11] The IEEE 802.3 protocol is described in RFC 3580, a copy of which was submitted with an Information Disclosure Statement previously filed by the Applicant. The IEEE 802.3 protocol is not the same as the IEEE 802.1X protocol. Kanuri et al. does not disclose the IEEE 802.1X protocol, nor does it disclose the IEEE 802.3 protocol in the context of user authentication. For this additional reason, the 35 U.S.C. § 103 rejection of Claim 3 is unsupported by the cited art of record and the rejection must be withdrawn.

Claim 4

Claim 4 recites:

> The network access device of claim 1, wherein the user policy identifies an access control list.

---

[10] Office Action at p. 8.

[11] P. Congdon et al., *RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*, September 2003, at § 1.

The Examiner states,

> ... Kanuri et al fails to disclose network access device wherein the user policy identifies an access control list. . However, Tsuchiya et al discloses network access device wherein the user policy identifies an access control list (Col 3, starting at line 36; IEEE 802.3.[12]

The Applicant respectfully disagrees. The cited portion of Tsuchiya et al. says nothing about an access control list, let alone wherein the user policy identifies an access control list as required by Claim 4. For this additional reason, the 35 U.S.C. § 103 Rejection of Claim 4 is unsupported by the cited art of record and the rejection must be withdrawn.

Claim 5

Claim 5 recites:

> The network access device of claim 1, wherein the user policy includes an access control list.

The Examiner states:

> ... Tsuchiya et al discloses the network access device wherein the user policy includes an access control list (Col2, starts at line 32; sending and receiving information according to the control table).[13]

The Applicant respectfully disagrees. The cited portion of Tsuchiya et al. says nothing about an access control list, let alone wherein the user policy includes an access control list as required by Claim 5. For this additional reason, the 35 U.S.C. § 103 Rejection of Claim 5 is unsupported by the cited art of record and the rejection must be withdrawn.

[12] Office Action, p. 8.
[13] Office Action at p. 8.

The Second 35 U.S.C. § 103 Rejection

Claims 35-43 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kanuri et al. in view of Short et al., further in view of Tsuchiva et al., and further in view of Volpano,[14] of which no claims are independent claims.[15] This rejection is respectfully traversed.

Claims 35-37

Claims 35, 36, and 37 depend from Claims 1, 13, and 23, respectively. The arguments made above with respect to the 35 U.S.C. § 103 rejection of independent Claims 1, 13, and 23 apply here as well. The 35 U.S.C. § 103 rejection of Claims 1, 13, and 23 is unsupported by the cited art of record because each and every element as set forth in Claims 1, 13, and 23 is not taught or suggested by Kanuri et al. in view of Short et al., and further in view of Tsuchiva et al. Accordingly, the 35 U.S.C. § 103 rejection of dependent claims 35-37 based on Kanuri et al. in view of Short et al., further in view of Tsuchiva et al., and further in view of Volpano is also unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claims 38, 40, and 42

Claims 38, 40, and 40 include limitations similar to Claims 1, 13, and 23, respectively. The arguments made above with respect to the 35 U.S.C. § 103 rejection of independent Claims 1, 13, and 23 apply here as well. The 35 U.S.C. § 103 rejection of Claims 1, 13, and 23 is unsupported by the cited art of record because each and every element as set forth in Claims 1, 13, and 23 is not taught or suggested by Kanuri et al. in view of Short et al., and further in view

[14] U.S. Patent No. 7,188, 634 to Volpano.
[15] Office Action at ¶ 9.

of Tsuchiva et al. Accordingly, the 35 U.S.C. § 103 rejection of claims 38, 40, and 42 based on Kanuri et al. in view of Short et al., further in view of Tsuchiva et al., and further in view of Volpano is also unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Claims 39, 41, and 43

Claims 39, 41, and 43, depend from Claims 38, 40, and 42, respectively. Claims 38, 40, and 42 being allowable, Claims 39, 41, and 43 must also be allowable for at least the same reasons as for Claims 38, 40, and 42.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-3557.

Respectfully submitted,

NIXON PEABODY LLP

Dated: December 1, 2008

/John P. Schaub/
John P. Schaub
Reg. No. 42,125

NIXON PEABODY LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040